Assignment 3: The Kernel Crypto API

CS 444: Operating Systems II

Fall 2016

Abstract

This project involves researching and implementing a RAM Disk Device driver which allocates memory that is encrypted on write and unencrypted on read. The goal is to gain an understanding of how RAM Drivers and Encryption works inside of an operating system. Through work our process of learning and implementing the RAM Driver is shown.

Joshua D. Bowen
Chris J. Mendez

November 14, 2016

Assignment 3, CS444 Christopher Mendez, Joshua Bowen

1 RAM Driver Design

After reading some of the LDD3 document linked to from the assignment, we went online and found a version of the sbull ram disk driver. The plan from there was to modify it and encrypt it accordingly. The majority of the changes to the driver occurred in the transfer function, which takes care of reading and writing to and from the ram disk. The original write used memcpy and we overwrote with:

memset(dev-¿data + offset + i, 0, cryptoi_cipher_blocksize(tfm));

crypto_cipher_encrypt_one(tfm, dev-¿data + offset + i, buffer + i);

Where tfm (which stands for transformation) is the cipher we defined using our key. Similarly the read originally used a memcpy to read the data, and we replaced that with:

crypto_cipher_decrypt_one(tfm, buffer + i, dev-¿data + offset + i);

2 Questions

2.1 What do you think the main point of this assignment is?

The main point of this assignment was to teach us more about different aspects of the kernel. Specifically pertaining to modules. Additionally due to the lack of our access to SUDO we learned how to problem solve and work our way around a problem to still arrive at the solution. In a very literal sense we did the problem solving associated with engineering.

2.2 How did you personally approach the problem? Design decisions, algorithm, etc.

Before we jumped into the problem it was incredibly important that we familiarized ourself with I/O. We began by researching this topic and reviewing what we already knew. From there we moved into the crypto library to familiarze ourself with that piece of software. We wanted to make sure we had an understanding of everything before we jumped intt it. After this we looked into stuff already existent within the Kernel.

Once we had found what we need we made the modifications that suited our needs. After we had exactly what we needed the testing phase begins. Our goal of course is to make sure that the program is doing eactly what we think it should be doing exactly when it should be doing it withour fail. Once the program was working properly then we would know it was done. If it was not working properly then we would further debug and if neccessary revist our implemtnation or solution and start again.

2.3 How did you ensure your solution was correct? Testing details, for instance.

To test our solution, we would output the data from the buffer three times. First, before it was encrypted, second after it was encrypted and third after it had been decrypted. If the output from before encryption and after decryption was the same and after being encrypted the output was gibberish, we knew our key was working.

2.4 What did you learn?

I learned some of the linux/crypto.h api, as well as the basics of a module in linux. Particularly we had to pass our key as a module parameter, which caused some issues in figuring that out. More broadly I feel like were beginning to grasp I/O to a greater degree and what goes into making it work in the kernel after doing two assignments involving I/O.

3 History

3.1 Git Version Control Log

Commit	Message
commit 475cc829ba05ad1c73607ff434ec9c2ef6dd8b81 Merge: 3e0482b 1b77c30 Author: bowenjos ¡bowenjos@oregonstate.edu¿ Date: Mon Nov 14 13:01:28 2016 -0800	Merge branch 'master' of https://github.com/bowenjos/cs444-020
commit 3e0482b935f3c650912424576c36879b2fd76b6b Author: bowenjos ¡bowenjos@oregonstate.edu¿ Date: Mon Nov 14 13:00:53 2016 -0800	Assignment3 Files

3.2 Work Log

Date	Time	What
11/08/2016	3pm-5pm	Started assignment, started looking into LDD3 and linux/crypto.h library to try to understand the api we would be using. Found out about the sbull driver and found a copy online.
11/10/2016	10am-12am	Began programming, created a key and a cipher and overwrote the transfer function.
11/11/2016	12am-2pm	Began write up.
11/12/2016	2pm-5pm	Worked on debugging the code, realized that the key needed to be passed as a module parameter.
11/13/2016	8am-10am	Continued writeup and debugging, understood the programming but am having difficulty getting the assignment to load as a module in a running vm.
11/13/2016	6pm-7pm	Continued write up, formatted written material into a LaTeXdocument.
11/14/2016	1pm-4pm	Finished write up.